TILS 1392

b&w-voorstel

GEMEENTE WEERT

Afdeling	: D&I - Dienstverlening & Informatie		B&W-voorstel: DJ-479334
Naam opsteller voorstel	: Harrie van Helvoort (0621876848)		Zaaknummer: 479333
Portefeuillehouder	: A.A.M.M. (Jos) Heijmans		Publicatie: Openbaar

Onderwerp

Collegeverklaring Eenduidige Normatiek & Single Information Audit (ENSIA) 2017.

Voorstel

De Collegeverklaring ENSIA 2017 te ondertekenen.

Inleiding

Gemeenten moeten door middel van een audit/zelf-evaluatie kunnen aantonen dat de 'systemen' die digitaal in verbinding staan met de buitenwereld, voldoen aan bepaalde veiligheidsnormen. Voor het jaar 2017 geldt dit voor de DigiD aansluitingen van de gemeente en het elektronisch berichtenverkeer tussen Suwinet en haar afnemers. De ENSIA methodiek wordt hiervoor gehanteerd.

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent voor gemeenten eenmalige informatieverstrekking en eenmalige IT-audit.
ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken, de VNG, gemeenten, het ministerie van Sociale Zaken & Werkgelegenheid en het ministerie van Infrastructuur & Milieu.

Per 2017 is het vanuit ENSIA verplicht om tijdens de jaarlijkse ENSIA audit (27 maart 2018) een verklaring te hebben van het college waarin vastgelegd is wat de status is van de maatregelen t.a.v. informatiebeveiliging en privacy.

Beoogd effect/doel

Aantonen bij de ENSIA Audit dat de gemeente in control is t.a.v. informatiebeveiliging en privacy.

Weert, 5 maart 2018	S		B	W FvE	W PS	W GG	W MvdH
De directeur		akkoord					
		bespreken					

Soort besluit: Besluit college 20032018

In te vullen door het B&W secretariaat:

☒ Akkoord
☐ Akkoord met tekstuele aanpassing door portefeuillehouder
☐ Anders, ni.:

☐ Niet akkoord
☐ Gewijzigde versie

☐ A-stuk
☐ B-stuk
☐ C-stuk

Beslissing d.d.: 20-03-2018 Nummer: 8

De secretaris,

Totaal aantal pagina's: 2
Pagina 1

Argumenten

Met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. Deze baseline is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.

Kanttekeningen en risico's

De Collegeverklaring maakt onderdeel uit van de jaarlijkse ENSIA Audit.

Financiële, personele en juridische gevolgen

Geen.

Uitvoering/evaluatie

De horizontale verantwoording bestaat uit de zelfevaluatie (zie bijlagen), een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag.

Communicatie/participatie

Raad informeren via de TILS-lijst

Overleg gevoerd met

Intern:

J. Steijvers (DigiD Beheerder Publiekszaken),
R. van Leeuwen, (DigiD beheerder WIZ),
M. C. van Dijk (DigiD beheerder Enabl-U),
T. Willems (SUWI Security Coördinator)

Extern:

Arjan Hassing (IT Auditter; 3Angles)

Bijlagen:

Collegeverklaring Eenduidige Normatiek & Single Information Audit (ENSIA) 2017
Rapportage-DigiD-Assessment-2017-Weert-1
Rapportage-DigiD-Assessment-2017-Weert-2
Rapportage-DigiD-Assessment-2017-Weert-3
Bijlage Suwinet Collegeverklaring ENSIA 2017

GEMEENTE WEERT

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Weert legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigID (aansluitnummers 571063, 1001325, 1002287) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1,2,3 DigiD) en Suwinet (bijlage 4 Suwinet) geïnformeerd over de afwijkingen van de normen. In geen van de gevallen zijn afwijkingen geconstateerd.

Verklaring college

Het college verklaart dat bij gemeente Weert op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID en Suwinet.

Weert, 20 maart 2018

College van B en W gemeente Weert,

G. Brinkman

secretaris

A.A.M.M. Heijmans

burgemeester

GEMEENTE WEERT

DigiD aansluiting no.1 - Bijlage B + C

Gemeente Weert

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	Ja
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	3 assessmentplichtige DigiD aansluitingen

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	571063
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	GEMEENTE WEERT1
Externe infrastructuur-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers: Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	SIMgroep
TPM datum: Voer hier de datum in van het TPM rapport.	29-11-2017
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Ja
Naam leverancier: Geef de naam op van de applicatieleverancier.	SIMgroep
TPM datum: Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	29-11-2017
TPM kenmerk: Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	Referentie 2017.277
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier: Geef de naam op van de SaaS-leverancier.	SIMgroep
TPM datum: Voer hier de datum in van het TPM rapport.	29-11-2017
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	Referentie 2017.277
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid: Leveren alle leveranciers een TPM op?	Ja

Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	
Reikwijdte TPM: Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM: Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja
Reikwijdte TPM: Zijn de TPM's maximaal 1 jaar oud?	Ja
Reikwijdte TPM: Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM: Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Nee
Externe auditor bedrijf: Vul de namen in van het bedrijf van de externe auditors:	3angles B.V.
Externe auditor: Vul de namen in van de externe auditors:	Arjan Hassing
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Nee
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	Geen

Bijlage B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 571063 en GEMEENTE WEERT1.

Gemeente Weert biedt de volgende functionaliteit aan waarvoor DigiD aansluiting DIGID KOPPELING voor authenticatie wordt gebruikt: eFormulieren van de SIMGroep via de gemeentelijke website. Deze functionaliteit wordt geboden door de volgende webapplicatie: Internet Gemeente Weert

Deze applicatie is een combinatie van maatwerk en standaard software en wordt onderhouden door Seneca

Deze applicatie is extern benaderbaar via de volgende URL(s): www.weert.nl. De infrastructuur waar deze applicaties op draaien wordt beheerd door Seneca in de vorm SaaS.

Het object van onderzoek was de webomgeving van DigiD aansluiting DIGID KOPPELING ('DigiD webomgeving'). Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius. Het onderstaande schema toont de webomgeving die is onderzocht door middel van een infrastructurele test.

Gemeente Weert heeft een deel DigiD webomgeving uitbesteed aan SIMgroep. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen

waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.

Bijlage C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van Gemeente Weert

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 571063 en GEMEENTE WEERT1.

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst[AB1]: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.
Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van Third Party Mededeling, SIMgroep, Referentie 2017.277, Haarlem, 29 november 2017 ondertekend door Drs. M. C. Dusink RE.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van Third Party Mededeling, SIMgroep, Referentie 2017.277, Haarlem, 29 november 2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/ niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet /niet van toepassing	Referentie/ rapportnummer
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet Voldoet Voldoet	Referentie 2017.277 Referentie 2017.277 Referentie 2017.277	Nee	Voldoet	
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van	Voldoet Voldoet Voldoet	Referentie 2017.277 Referentie 2017.277 Referentie 2017.277	Ja	Voldoet	

	rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.					
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet Voldoet	Referentie 2017.277 Referentie 2017.277 Referentie 2017.277	Ja	Voldoet	
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.		Referentie 2017.277 Referentie 2017.277Referentie 2017.277			
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet Voldoet Voldoet	Referentie 2017.277 Referentie 2017.277 Referentie 2017.277	Ja	Voldoet	
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.		Referentie 2017.277 Referentie 2017.277 Referentie			

			2017.277			
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
C.03	Vulnerability assesments (security scans) worden		Referentie 2017.277 Referentie 2017.277			

	procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).		Referentie 2017.277			
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.		Referentie 2017.277 Referentie 2017.277 Referentie 2017.277			
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet Voldoet Voldoet	Referentie 2017.277 Referentie 2017.277 Referentie 2017.277	Ja	Voldoet	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig		Referentie 2017.277 Referentie 2017.277 Referentie			

	uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.		2017.277			

GEMEENTE WEERT

DigiD aansluiting no.2 - Bijlage B + C

Gemeente Weert

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	1001325
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	DIGITAAL LOKET
Externe infrastructuur-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers: Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	PinkRoccade
TPM datum: Voer hier de datum in van het TPM rapport.	27-09-2017
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Ja
Naam leverancier: Geef de naam op van de applicatieleverancier.	PinkRoccade
TPM datum: Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	27-09-2016
TPM kenmerk: Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	Rapportnummer: AQR9LV
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier: Geef de naam op van de SaaS-leverancier.	PinkRoccade
TPM datum: Voer hier de datum in van het TPM rapport.	27-09-2016
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	Rapportnummer: AQR9LV
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid: Leveren alle leveranciers een TPM op?	Ja
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	
Reikwijdte TPM: Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM: Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja
Reikwijdte TPM: Zijn de TPM's maximaal 1 jaar oud?	Ja

Reikwijdte TPM: Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM: Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Ja
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	Rapportnummer: AQR9LV
Externe auditor: Vul de namen in van de externe auditors:	Arjan Hassing
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Nee
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	Geen

Bijlage B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 1001325 en DIGITAAL LOKET.

Gemeente Weert heeft een deel DigiD webomgeving uitbesteed aan PinkRoccade Local Government. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.

Bijlage C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van [gebruikersorganisatie]

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 1001325 en DIGITAAL LOKET.

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van Third party-mededeling DigiD, PinkRoccade Local Government B.V., Rapport voor Gemeente Weert, Datum uitgifte rapport: 27 september 2017 ondertekend door ir. J.G.G.V. van den Boom RE.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van Third party-mededeling DigiD, PinkRoccade Local Government B.V., Rapport voor Gemeente Weert, Datum uitgifte rapport: 27 september 2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij	Referentie/ rapportnummer	Aanvullende beheersmaatre	Getoetst bij	Referentie/ rapportnu

		leverancier: Voldoet niet/Voldoet/ niet van toepassing		gelen gebruikersorganisatie Ja/Nee	gebruiker Voldoet niet/Voldoet/niet van toepassing	mmer
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet Voldoet Voldoet	Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV	Ja	Voldoet	
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Voldoet Voldoet Voldoet	Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV	Ja	Voldoet	
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet Voldoet	Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV	Ja	Voldoet	
U/WA	De webapplicatie		Rapportnummer:			

.03	beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.		AQR9LV Referentie 2017.277Rapport nummer: AQR9LV			
U/WA .04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/WA .05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet Voldoet Voldoet	Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV	Ja	Voldoet	
U/PW .02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/PW .03	De webserver is ingericht volgens een configuratie-baseline.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/PW .05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/PW .07	Voor het configureren van platformen een		Rapportnummer: AQR9LV Referentie			

	hardeningsrichtlijn beschikbaar.		2017.277 Rapportnummer: AQR9LV			
U/NW .03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/NW .04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/NW .05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
U/NW .06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen,		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			

	uitgevoerd op de infrastructuur van de webapplicatie (scope).					
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.		Rapportnummer: AQR9l V Referentie 2017.277 Rapportnummer: AQR9LV			
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet Voldoet Voldoet	Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV	Ja	Voldoet	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.		Rapportnummer: AQR9LV Referentie 2017.277 Rapportnummer: AQR9LV			

Dit hoofdstuk is niet voor u van toepassing.

GEMEENTE WEERT

DigiD aansluiting no.3 - Bijlage B + C

Gemeente Weert

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	1002287
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	PIP
Externe infrastructuur-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers: Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	Pink Roccade
TPM datum: Voer hier de datum in van het TPM rapport.	17-02-2017
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Ja
Naam leverancier: Geef de naam op van de applicatieleverancier.	pink roccade
TPM datum: Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	17-02-2017
TPM kenmerk: Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	AAS2017-159
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier: Geef de naam op van de SaaS-leverancier.	pink roccade
TPM datum: Voer hier de datum in van het TPM rapport.	17-02-2017
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	AAS2017-159
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid: Leveren alle leveranciers een TPM op?	Ja
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	
Reikwijdte TPM: Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM: Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja
Reikwijdte TPM: Zijn de TPM's maximaal 1 jaar oud?	Ja

Reikwijdte TPM: Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM: Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Ja
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	AAS2017-159
Externe auditor: Vul de namen in van de externe auditors:	Arjan Hassing
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Nee
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	Geen

Bijlage B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 1002287 en PIP.

Gemeente Weert heeft een deel DigiD webomgeving uitbesteed aan PinkRoccade Local Government. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.

Bijlage C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van [gebruikersorganisatie]

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 1002287 en PIP.

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van ICT-beveiliginsassessment DigiD applicatie PIP, AAS2017-159, 17 februari 2017 ondertekend door P.C.M. Holierhoek RE RA.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van ICT-beveiliginsassessment DigiD applicatie PIP, AAS2017-159, 17 februari 2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet /niet van	Referentie/ rapportnummer

		niet/Voldoet/ niet van toepassing			toepassing	
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet Voldoet Voldoet	AAS2017-159 Referentie 2017.277 AAS2017-159	Ja	Voldoet	
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Voldoet Voldoet Voldoet	AAS2017-159 Referentie 2017.277 AAS2017-159	Ja	Voldoet	
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet Voldoet	AAS2017-159 Referentie 2017.277 AAS2017-159	Ja	Voldoet	
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt		AAS2017-159 Referentie 2017.277AAS 2017-159			

	verwerkt.					
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderen de en cryptografische technieken.	Voldoet Voldoet Voldoet	AAS2017-159 Referentie 2017.277 AAS2017-159	Ja	Voldoet	
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.		AAS2017-159 Referentie 2017.277 AAS2017-159			

U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		AAS2017-159 Referentie 2017.277 AAS2017-159			
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.		AAS2017-159 Referentie 2017.277 AAS2017-159			
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).		AAS2017-159 Referentie 2017.277 AAS2017-159			
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).		AAS2017-159 Referentie 2017.277 AAS2017-159			
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.		AAS2017-159 Referentie 2017.277 AAS2017-159			
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de		AAS2017-159 Referentie 2017.277 AAS2017-159			

	beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.					
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet Voldoet Voldoet	AAS2017-159 Referentie 2017.277 AAS2017-159	Ja	Voldoet	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.		AAS2017-159 Referentie 2017.277 AAS2017-159			

Bijlage 2 Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging Suwinet van de gemeente Weert.

<in geval van gebruik van Suwinet voor niet-SUWI-taken waarbij een overeenkomst conform Regeling SUWI bijlage 3 Aansluitprotocol is afgesloten: Naast het gebruik van Suwinet voor wettelijke SUWI-taken heeft de gemeente voor de volgende taken (een) overeenkomst(en) afgesloten conform Regeling Suwi bijlage 3 Aansluitprotocol GeVS voor het gebruik van Suwinet als niet-SUWI-partij:

- ...
- ...

Het gebruik van Suwinet als niet-SUWI-partij is onderdeel van de Collegeverklaring. >
<De gemeente heeft de volgende taken <geheel of gedeeltelijk> uitbesteed aan <organisatie>. De uitbestede taken zijn onderdeel van de Collegeverklaring omdat wij voor de uitbestede taken de volledige verantwoordelijkheid dragen.>

Afwijkingen van de normen
Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

- BIG:<BIG-nummer> / Suwinet: <Suwinet-nummer> <Suwinet-Inkijk of naam inleesapplicatie en DKD-Inlezen/Suwinet-Inlezen>.
- ...

<ingeval niet-SUWI-taken: Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de niet-SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

- BIG:<BIG-nummer> / Suwinet: <Suwinet-nummer> <Suwinet-Inkijk of Suwinet/DKD-inlezen en naam inleesapplicatie>.

...>